UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,585	10/24/2003	Klaus U. Schutz	MS1-1819US	1086

22801 7590 02/06/2008
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
COLAN, GIOVANNA B	
ART UNIT	**PAPER NUMBER**
2162	
MAIL DATE	**DELIVERY MODE**
02/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/693,585	**Applicant(s)** SCHUTZ ET AL.	
	Examiner Giovanna Colan	**Art Unit** 2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 November 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-14,17-23,32 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-14,17-23,32 and 33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is issued in response to the Amendment filed on 11/12/2007.

2. Claims 9, 12 – 13, 17 – 20, and 22 – 23 were amended. Claims 1 – 8, 15 – 16, and 24 – 32 were canceled. Claim 33 was added.

3. This action is made Final.

4. Claims 9 – 14, 17 – 23, and 32 – 33 are pending in this application.

5. Applicant's arguments with respect to previously presented and/or amended limitations filed on 11/12/2007 have been fully considered but they are not persuasive.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 9 – 11, 13 – 14, 17 – 19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Botz et al. (Botz hereinafter) (US Patent App. Pub. No. 2003/0177388 A1, filed: March 15, 2002) in view of Kao et al. (Kao hereinafter) (US Patent No. 6,651,168 B1, filed January 29, 1999).

Regarding Claim 9, Botz discloses a method comprising:

receiving a credential from a user at an input device in communication with a local machine having a native operating system (OS) (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 11, Botz[1]).

Botz also discloses a plurality of input devices (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz). However, Botz does not explicitly disclose a plurality of different input devices. On the other hand, Kao discloses: the local machine capable of being in communication with a plurality of different input devices each configured to enable the user to log on with the native OS to access the local machine (Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Kao's teachings to the system of Botz. Skilled artisan would have been motivated to do so, as suggested by Kao (Col. 2, lines 25 – 28, Kao), to provide a flexible way to provide diverse user authentication mechanisms and processes for a stand alone computer system or for a computer network. In addition, both of the references (Botz and Kao) teach features that are directed to analogous art and they are directed to the same field of endeavor, such as, databases management systems, receiving credentials, and authentication. This close relation between both of the references highly suggests an expectation of success.

Furthermore, the combination of Botz and Kao discloses:

translating the credential with one of a plurality of different coexisting credential provider modules for translating respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine (Page 1, [0007], lines 13 – 17, Botz[2]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao); and the plurality of different coexisting credential provider modules also enabling the user to log on with the native OS to access the local machine with each corresponding different input device that is in communication with local machine (Fig. 13, items 1402, 1404, and

[1] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[2] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

communicating the translated credential having the common credential protocol through a credential provider Application Program Interface (API) to a logon user interface (UI) routine of the native OS, wherein the credential provider API is configured to interface with each of the plurality of different coexisting credential provider modules (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

passing the translated credential having the common credential protocol to a logon routine of the OS from the logon UI routine (Page 1, [0007], lines 13 – 17, Botz; and Col. 9, lines 24 – 27, Kao);

calling the logon routine for the native OS to authenticate the translated credential having the common credential protocol against a credential database (Page 1, [0008], lines 6 – 9, Botz; and Col. 9, lines 24 – 27, Kao); and logging the user on with the native OS to access the local machine when the authentication is successful (Page 3, [0034], lines 7 – 13, Botz[3]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao).

Regarding Claim 10, the combination of Botz in view of Kao discloses a method, wherein the logging of the user on further comprises logging the user on to the local machine after a plurality of said credentials have been received, translated by a respective said different coexisting credential provider module, and authenticated successfully (Page 7, [0094], lines 6 – 10, wherein the identity of the initial authentication server, identity of the user, etc in [0099] - [0106] corresponds to the plurality of the credentials as claimed, Botz; and Col. 17, lines 23 – 26, Kao, Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao, and also Col. 8, lines 64 – 67 , " a smart card 222 is plugged into the smart card reader 220 and a user's DCE ID and password is stored in the smart card...", Kao).

Regarding Claim 11, the combination of Botz in view of Kao discloses a method, wherein the user is not logged on to the local machine at the time when the translated credentials are authenticated (Page 7, [0094], lines 6 – 10, Botz).

Regarding Claim 13, the combination of Botz in view of Kao discloses a method, wherein each said credential provider module is interoperable, through a credential

[3] Wherein the step of sign-on corresponds to the step of logging the user claimed.

provider API, to the component of the native OS (Fig. 4, item 402, Page 5, [0071], lines 1 – 4, the interfaces services, Botz).

Regarding Claim 14, the combination of Botz in view of Kao discloses a computer-readable medium comprising instructions that, when executed by a computer (Page 2, [0030], lines 1 – 4, Botz).

Regarding Claim 17, the combination of Botz in view of Kao discloses a method comprising:

receiving a credential from a user at an input device in communication with a local machine having a native operating system (OS) (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 11; respectively, Botz[4]), the local machine capable of being in communication with a plurality of different input devices, each capable of receiving a credential from the user to enable the user to log on to access the local machine with the native OS (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

translating the credential with a credential provider module that corresponds to the input device (Page 1, [0007], lines 13 – 17, Botz[5]; and Fig. 1, item 200, Col. 8, lines

[4] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[5] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao), wherein:

the credential provider module is one of a plurality of coexisting different said credential provider modules (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao); and

each said credential provider module can perform a translation of a respectively different type of said credential received at a different said input device in communication with the local machine (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, Kao); and

each said translation of each said credential is in a common credential protocol, the common credential protocol being compatible with the native OS of the local machine (Page 1, [0007], lines 13 – 17, Botz[6]; and (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, Kao);

[6] Wherein the local user identity corresponds to the common credential protocol claimed.

communicating the translated credential having the common credential protocol through a credential provider interface to a logon user interface (UI) routine of the native OS, wherein the credential provides interface is configured to interface with each of the plurality of coexisting different said credential provider modules (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

passing the translated credential having the common credential protocol to a logon routine of the native OS from the logon UI routine (Page 1, [0007], lines 13 – 17, Botz; and Col. 9, lines 24 – 27, Kao);

authenticating the translated credential against a credential database with the logon routine of the native OS (Page 1 and 7, [0008] and [0092], lines 6 – 9 and 1 – 5; respectively, Botz[7]; and Col.9, lines 1 – 7, Kao); and

logging the user on to access the local machine with the native OS when the authentication is successful (Page 3, [0034], lines 7 – 13, Botz[8]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao).

[7] Wherein the step of performing subsequent authentication corresponds to the step of authenticating claimed.

[8] Wherein the step of sign-on corresponds to the step of logging the user claimed.

Regarding Claim 18, the combination of Botz in view of Kao discloses a method, wherein the logging the user on to access the local machine with the native OS further comprises deferring the logging on of the user to access the local machined until the receiving, the translating, the communicating, the passing, and the authenticating successfully have been repeated for each of a plurality of said credentials (Page 7, [0094], lines 6 – 10, Botz[9]).

Regarding Claim 19, the combination of Botz in view of Kao discloses a method, wherein the user is not logged on to access the local machine when the translated credentials are authenticated against the credential database with the logon routine of the native OS (Page 7, [0094], lines 6 – 10, Botz).

Regarding Claim 21, the combination of Botz in view of Kao discloses a computer-readable medium comprising instructions that, when executed by a computer, perform the method of claim 17 (Page 2, [0030], lines 1 – 4, Botz).

Regarding Claim 22, the combination of Botz in view of Kao discloses a computer-readable medium comprising a credential provider module including

[9] Wherein the step of using the policy information, including trust policy and initial authentication, to signing the user on (Page 7, [0094], lines 1 – 6, Botz) corresponds to the step of logging the user claimed. In addition, Botz discloses the use of a plurality of credentials as claimed (Page 7, [0101], lines 3 – 14, Botz). By signing the user on after the information is authenticated, the system is deferring the signing on or logging on.

instructions that, when executed by a local machine having a native operating system OS, receive and translate a credential into a credential protocol so as to be compatible for authentication by an authentication component of the native OS against a credential database for logging a user identified by the credential on with the native OS to access the local machine when the authentication is successful, wherein:

the translated credential is received via a credential provider Application Programming Interface (API) of the authentication component of the native OS (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

the credential provider API (Fig. 3, items 314, and 316, Page 4, [0058], lines 1 – 4, Botz) of the authentication component of the native OS is compatible for receiving each of a plurality of said credentials (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 13; respectively; wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed; Botz) from a corresponding plurality of different coexisting credential provider modules (Page 1 and 4, [0007] and [0050], lines 13 – 17 and 1 – 6, multiple security user registries of multiple computer platforms; respectively, Botz; and

Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, Kao); and

each said different coexisting credential provider module can:

receive a respective different type of said credential from a respective input device (Fig.10, items 1104, 1108, 1110, and 1112, Page 9, [0123], lines 8 – 11, Botz[10]), each respective input device capable of coupling to the local machine and enabling the user to log on with the native OS to access the local machine (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao); and

translate each said different type of said credential into the credential protocol so as to be compatible for authentication by the authentication component of the native OS against the credential database (Page 3, [0039], lines 1 – 6, an infrastructure to support run-time cooperation between disparate security registry user, Botz; and Page 1, [0007], lines 13 – 17, Botz[11]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation

[10] Wherein examiner interprets the step where a first user signs on using Public Key infrastructure (PKI), and a second user signs on using Kerberos (Page 9, [0123], lines 8 – 11, Botz) as the step of receiving different type of credential from respective input device as claimed.

[11] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

function implementation converts these data attributes to determine the style or format ...", Kao).

Regarding Claim 33, the combination of Botz in view of Kao discloses a method comprising:

receiving a credential from a user at an input device in communication with a local machine having a OS (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 11; respectively, Botz[12]), the local machine capable of being in communication with a plurality of different input devices each configured to enable the user to log on with the OS to access local machine (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

translating the credential with one of a plurality of different coexisting credential provider modules for translating respectively different types of credentials into a common credential protocol (Page 1, [0007], lines 13 – 17, Botz[13]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao), the plurality of different

[12] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[13] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

coexisting credential provider modules also enabling the user to log on with the OS to access the local machine with each corresponding different input device that is in communication with local machine (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

using a component of the OS to authenticate the translated credential having the common credential protocol against a credential database; and

logging the user on with the native OS to access the local machine when the authentication is successful, wherein the logging of the user on further comprises logging the user on to the local machine after a plurality of said credentials have been received, translated by a respective said different coexisting credential provider module, and authenticated successfully (Page 7, [0094], lines 6 – 10, wherein the identity of the initial authentication server, identity of the user, etc in [0099] - [0106] corresponds to the plurality of the credentials as claimed, Botz; and Col. 17, lines 23 – 26, Kao, Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao, and also Col. 8, lines 64 – 67 , " a smart card 222 is plugged into the smart card reader 220 and a user's DCE ID and password is stored in the smart card...", Kao).

9. Claims 12, 20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Botz et al. (Botz hereinafter) (US Patent App. Pub. No. 2003/0177388 A1, filed: March 15, 2002), in view of Kao et al. (Kao hereinafter) (US Patent No. 6,651,168 B1, filed January 29, 1999), and further in view of Axel et al.

(Axel hereinafter) (US Patent App. Pub. No. 2004/0139355 A1, filed: November 7, 2002).

Regarding Claim 12, the combination of Botz in view of Kao discloses all the limitations as disclosed above including a method, wherein the use of the component of the native OS to authenticate the translated credential having the common credential protocol against the credential database further comprises:

communicating the translated credential to an LSA (Page 7, [0090], lines 1 – 5, Botz[14]); and

determining the authentication with the LSA against the credential database (Page 7, [0090], lines 6 – 9, Botz[15]) that is selected from the group consisting of:

a local database other than the SAM database (Page 5, [0069], lines 3 – 5, local user registry, Botz);

a remote credential database (Page 5, [0067], lines 12 – 14, LDAP-accessible storage, Botz[16]);

a token protocol credential service (Page 9, [0133], lines 2 – 6, HyperText Transfer Protocol (HTTP), Botz);

[14] Wherein examiner interprets the AIT domain controller as the LSA claimed; and the identity translation token (ITT) and/or the identity translation token reference (ITTR) as the translated credential claimed.

[15] Wherein the step of validating the translated token using a copy of the signing value retained at the AIT domain controller corresponds to the step of determining the authentication against the credential database as claimed. In addition, Botz further discloses that this controller utilizes databases to store the information (Page 6, [0086], lines 3 – 7, Botz).

[16] Wherein the LDPA-accessible storage corresponds to the remote credential database claimed. The reason is because this storage is retrieved upon a server session, which would imply a remote session.

a challenge and response protocol service (Page 9, [0133], lines 1 – 6, HyperText Transfer Protocol (HTTP), Botz[17]);

In addition, the combination of Botz in view of Kao further discloses KDC (Fig. 10, item 1102, Kerberos, Botz). However, the combination of Botz in view of Kao is silent with respect to a SAM database; and an AD at a domain remote from the local machine. On the other hand, Axel discloses a system including a SAM database (Page 2, [0018], lines 3 – 5, Axel); an AD (Page 2, [0017], lines 4 – 5, Axel) and KDC at a domain remote from the local machine (Page 2, [0017], lines 1 – 3, Axel); and an LSA (Page 2, [0021], lines 1 – 2, Axel). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Axel's teachings to the system of the combination of Botz in view of Kao. Skilled artisan would have been motivated to do so, as suggested by Axel (Page 1, [0002], lines 1 – 4, Axel), to provide access to various password-enabled computer network elements through the use of a single password enabled network element. In addition, the applied references (Botz, Kao, and Axel) teach features that are directed to analogous art and they are directed to the same field of endeavor of databases management systems, such as, authentication, and login users. This close relation between the applied references highly suggests an expectation of success.

[17] Wherein the feature of extracting corresponds to the challenge claimed; and the feature of passing corresponds to the response claimed.

Regarding Claim 20, the combination of Botz in view of Kao and further in view of Axel discloses a method, wherein the authenticating of the translated credential against the credential database with the logon routine of the native OS further comprises:

communicating the translated credential to an LSA from the logon routine of the native OS (Page 7, [0090], lines 1 – 5, Botz[18]; and Page 2, [0021], lines 1 – 2, LSA, Axel); and

determining the authentication with the LSA against the credential database (Page 7, [0090], lines 6 – 9, Botz[19]; and Page 2, [0021], lines 1 – 2, LSA, Axel) that is selected from the group consisting of:

a SAM database (Page 2, [0018], lines 3 – 5, Axel);

a local database other than the SAM database (Page 5, [0069], lines 3 – 5, local user registry, Botz);

a remote credential database (Page 5, [0067], lines 12 – 14, LDAP-accessible storage, Botz[20]);

a token protocol credential service (Page 9, [0133], lines 2 – 6, HyperText Transfer Protocol (HTTP), Botz);

a challenge and response protocol service (Page 9, [0133], lines 1 – 6, HyperText Transfer Protocol (HTTP), Botz[21]); and

[18] Wherein examiner interprets the AIT domain controller as the LSA claimed; and the identity translation token (ITT) and/or the identity translation token reference (ITTR) as the translated credential claimed.

[19] Wherein the step of validating the translated token using a copy of the signing value retained at the AIT domain controller corresponds to the step of determining the authentication against the credential database as claimed. In addition, Botz further discloses that this controller utilizes databases to store the information (Page 6, [0086], lines 3 – 7, Botz).

[20] Wherein the LDPA-accessible storage corresponds to the remote credential database claimed. The reason is because this storage is retrieved upon a server session, which implies a remote session.

an AD (Page 2, [0017], lines 4 – 5, Axel) and KDC at a domain remote from the local machine (Page 2, [0017], lines 1 – 3, Axel; and Fig. 10, item 1102, Kerberos, Botz).

Regarding Claim 23, the combination of Botz in view of Kao and further in view of Axel discloses a computer-readable medium, wherein the authentication component of the native OS comprises:

a logon user interface (UI) module (Page 6, [0076], lines 1 – 5, Botz; and Col. 8, lines 22 – 34, Kao);

an OS logon module for receiving Remote Procedure Call (RPC) calls from the logon UI module (Page 6, [0083], lines 1 – 5, remote sign-on, Botz; and Col. 8, lines 22 – 34, Kao); and

an LSA for determining the authentication, and in communication with, the credential database (Page 7, [0090], lines 6 – 9, Botz[22]) that is selected from the group consisting of:

a SAM database (Page 2, [0018], lines 3 – 5, Axel);

a local database other than the SAM database (Page 5, [0069], lines 3 – 5, local user registry, Botz);

[21] Wherein the feature of extracting corresponds to the challenge claimed; and the feature of passing corresponds to the response claimed.

[22] Wherein the step of validating the translated token using a copy of the signing value retained at the AIT domain controller corresponds to the step of determining the authentication against the credential database as claimed. In addition, Botz further discloses that this controller utilizes databases to store the information (Page 6, [0086], lines 3 – 7, Botz).

a remote credential database (Page 5, [0067], lines 12 – 14, LDAP-accessible storage, Botz[23]);

a token protocol credential service (Page 9, [0133], lines 2 – 6, HyperText Transfer Protocol (HTTP), Botz);

a challenge and response protocol service (Page 9, [0133], lines 1 – 6, HyperText Transfer Protocol (HTTP), Botz[24]); and

an AD (Page 2, [0017], lines 4 – 5, Axel) and KDC at a domain remote from the local machine (Page 2, [0017], lines 1 – 3, Axel; and Fig. 10, item 1102, Kerberos, Botz).

[23] Wherein the LDPA-accessible storage corresponds to the remote credential database claimed. The reason is because this storage is retrieved upon a server session, which implies a remote session.

Response to Arguments

1. Applicant argues that the applied art fails to disclose; "...logging the user on to the local machine after a plurality of said credentials have been received, translated by a respective said different coexisting credential provider module, and authenticated successfully".

Examiner respectfully disagrees. The applied art does disclose: logging the user on to the local machine after a plurality of said credentials have been received, translated by a respective said different coexisting credential provider module, and authenticated successfully (Page 7, [0094], lines 6 – 10, wherein the identity of the initial authentication server, identity of the user, etc in [0099] - [0106] corresponds to the plurality of the credentials as claimed, Botz; and Col. 17, lines 23 – 26, Kao, Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao, and also Col. 8, lines 64 – 67 , " a smart card 222 is plugged into the smart card reader 220 and a user's DCE ID and password is stored in the smart card...", Kao). To further clarify, the examiner has interpreted the claims in view of the specification. Since the specification defines the credentials as usernames, passwords, smart cards, etc ([0004] specification of the disclosure), the examiner has made the correspondence explained above.

[24] Wherein the feature of extracting corresponds to the challenge claimed; and the feature of passing

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Botz et al. (US Patent App. Pub. No. 2003/0177388 A1, filed: March 15, 2002) discloses authenticated identity translation within a multiple computing unit environment.

Axel et al. (US Patent App. Pub. No. 2004/0139355 A1, filed: November 7, 2002) discloses a method and system of accessing a plurality of network elements.

Hartman et al. (US Patent No. 6,807,636 B2) discloses methods and apparatus for facilitating security in a network.

Kao et al. (US Patent No. 6,651,168 B1, filed January 29, 1999).

2. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

corresponds to the response claimed.

Points Of Contact

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Giovanna Colan whose telephone number is (571) 272-2752. The examiner can normally be reached on 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Giovanna Colan
Examiner
Art Unit 2162
January 31, 2008

SHAHID ALAM
PRIMARY EXAMINER